What To Do AFTER You Get A New CAC?

A. Reboot/Restart the computer (this step is critical)

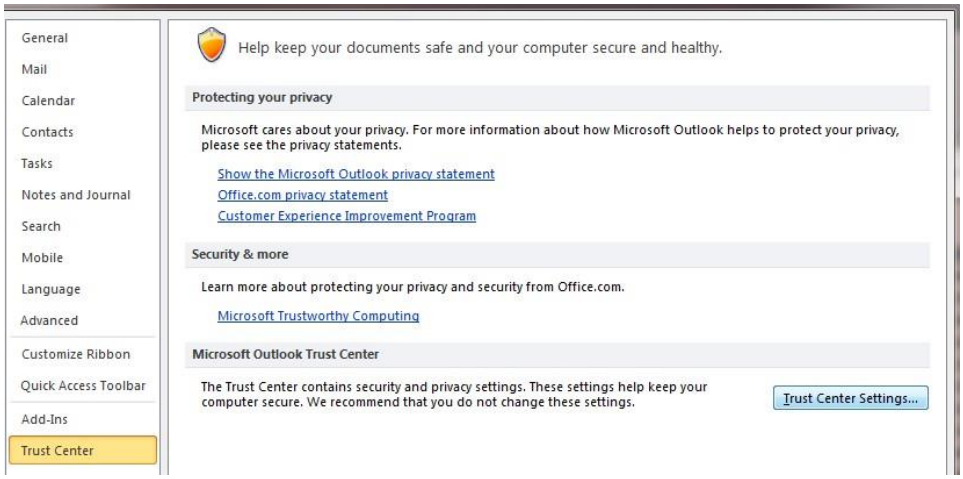
B. Log in with new CAC

C. After boot up process is complete, publish your certificates to the GAL:

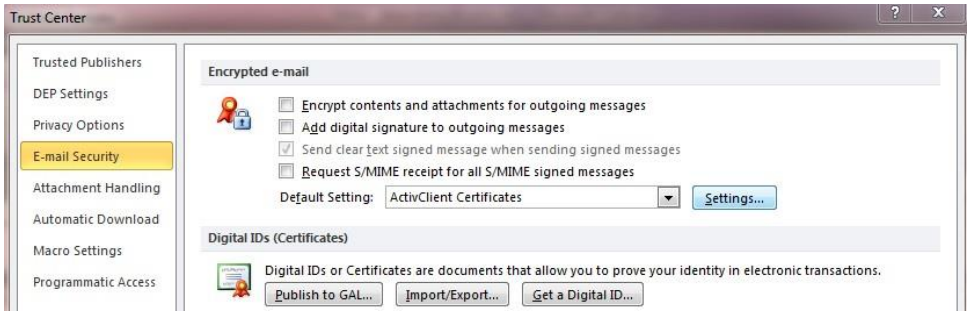
Publishing your certificates to the GAL (Global Address List)

Step: 1
Open MS Outlook -> choose “File” –> choose “Info” -> choose “Options”

Step: 2
Choose “Trust Center” -> “Trust Center Settings” ->

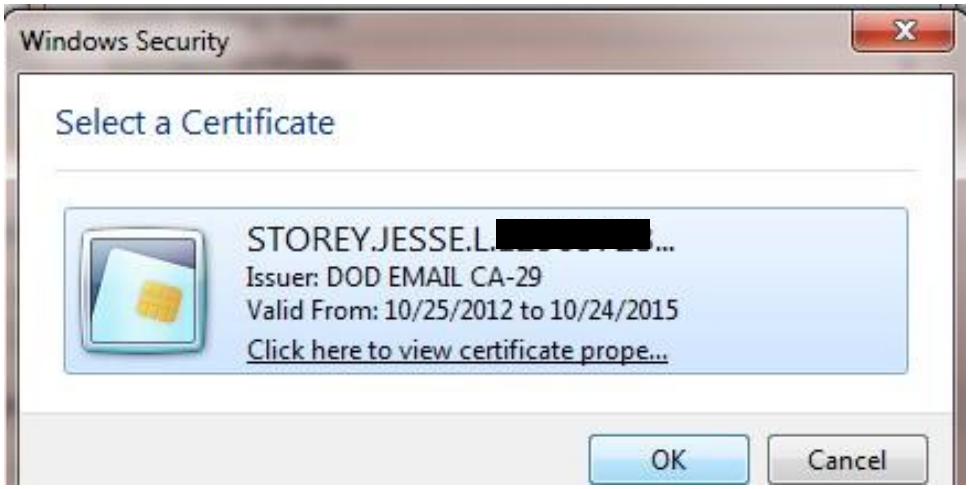


Step 3:
Choose “Email Security” -> Choose “Settings”

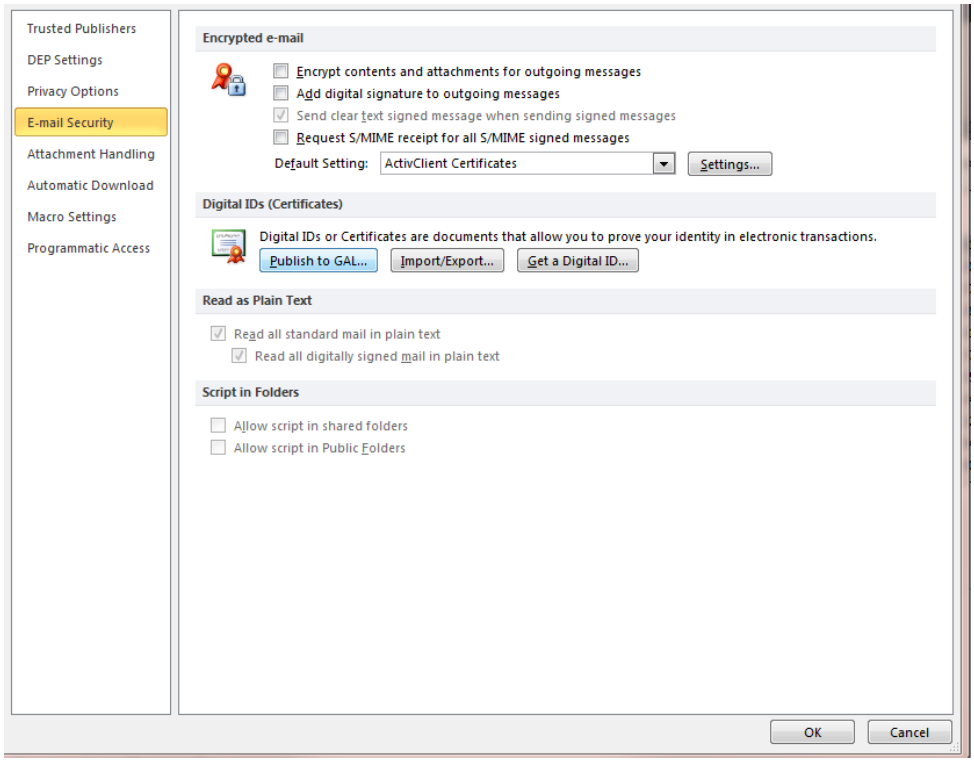


Step 4:
Choose “Settings” -> Choose “Choose (Signing)”-> Select the Newest/Latest Certificate -> Click “OK”

Step: 4
Choose “Settings” -> Choose “Choose”-> Select the Newest/Latest Certificate -> Click “OK”



Step 5:
Choose “Publish to Gal”



D. Make sure you can log in to AKO. Most Army websites authenticate through AKO-EAMS-A

E. If you have trouble logging in to a website after following these steps, you may need to register your CAC with the websites. Two examples of websites that require you to contact their help desk to register the new CAC certificate is LMP and LIW. There are other websites too.

F. Delete old certificates by launching Internet Explorer 11 and click on Tools/Internet Options and select the Content tab. *Only* delete personal certificates that are old or expired.

G. If you work with encrypted files or encrypted emails then you will need to recover your old certificates from the DoD Automated Key Recovery agent after they are deleted so that they can be stored in the proper certificate cache used for older personal certificates. The recover old certificates go here:
https://home.army.mil/samhouston/application/files/5115/5423/3563/CAC-AutomaticKeyRecoveryMar2017.pdf

Please contact your local IT Support organization if you require additional information or assistance.